



Broadband Access Center の監視

この章では、Broadband Access Center (BAC) 配備内の中央 RDU サーバおよび DPE サーバを監視する方法について説明します。次のトピックについて説明します。

- [イベントのロギング \(P.10-2\)](#)
- [SNMP の使用によるサーバの監視 \(P.10-10\)](#)
- [サーバ状態の監視 \(P.10-17\)](#)

イベントのロギング

イベントのロギングは RDU と DPE で実行されます。まれに、視認性向上のために、DPE イベントが RDU に記録されることもあります。

ログ ファイルはそれぞれのログ ディレクトリに保存され、任意のテキスト エディタを使用して調べることができます。ログ ファイルを圧縮すると、トラブルシューティングや障害の解決のために Cisco Technical Assistance Center またはシステム インテグレータに電子メールで送信しやすくなります。

また、RDU と DPE のログには、管理者のユーザ インターフェイスからアクセスすることもできます。

ログのレベルおよび構造

例 10-1 に示されているログ ファイル構造には、次のものが含まれます。

- Domain Name : ログ ファイルが生成されたコンピュータの名前。
- Date and Time : メッセージがログに記録された日時。ここでは、該当するシステムの時間帯も示されます。
- Facility : システムを識別します (この場合は BAC)。
- Sub-facility : BAC のサブシステムまたはコンポーネントを識別します。
- Severity Level : ログ システムが定義する、ログの問題を処理するときの緊急性を識別するために使用される 7 段階の重大度のレベル (表 10-1 を参照)。次の重大度のレベルの設定方法については、P.10-3 の「[重大度のレベルの設定](#)」を参照してください。

表 10-1 重大度のレベル

ログ レベル	説明
0 : 緊急	システムが不安定です。すべての緊急メッセージを保存するように、ロギング機能を設定します。
1 : アラート	すぐに対応が必要です。すぐに対応が必要なすべてのアクティビティ、およびさらに深刻な活動を保存するように、ロギング機能を設定します。
2 : クリティカル	クリティカルな状態が存在します。すべてのエラー メッセージ、およびさらに深刻なメッセージを保存するように、ロギング機能を設定します。
3 : エラー	エラー状態が存在します。すべてのエラー メッセージ、およびさらに深刻なメッセージを保存するように、ロギング機能を設定します。
4 : 警告	警告状態が存在します。すべての警告メッセージ、およびさらに深刻なメッセージを保存するように、ロギング機能を設定します。
5 : 通知	通常ですが、重大な状態が存在します。すべての通知メッセージ、およびさらに深刻なメッセージを保存するように、ロギング機能を設定します。
6 : 情報	情報メッセージ。利用可能なすべてのロギング メッセージを保存するように、ロギング機能を設定します。



(注) 7 (デバッグ) として知られるもう 1 つのレベルは、シスコでデバッグの目的にのみ使用されます。Cisco Technical Assistance Center から指示された場合を除き、このレベルは使用しないようにしてください。

- Msg ID : メッセージ テキストの固有な識別子。
- Message : 実際のログ メッセージ。

例 10-1 ログ ファイルのサンプル

Domain Name	Data and Time	Facility	Sub-facility	Severity Level	Msg ID	Message
bac.example.com:	2007 9 6 03:06:11 EST:	%BAC-	RDU-	5	0236:	Broadband Access Center Regional Distribution Unit starting up
bac.example.com:	2007 9 6 03:06:15 EST:	%BAC-	RDU-	5	0566:	Initialized API defaults
bac.example.com:	2007 9 6 03:06:15 EST:	%BAC-	RDU-	5	0567:	Initialized Network Registrar defaults
bac.example.com:	2007 9 6 03:06:15 EST:	%BAC-	RDU-	5	0568:	Initialized Server defaults
bac.example.com:	2007 9 6 03:06:18 EST:	%BAC-	RDU-	5	0570:	Initialized DOCSIS defaults
bac.example.com:	2007 9 6 03:06:18 EST:	%BAC-	RDU-	5	0571:	Initialized Computer defaults
bac.example.com:	2007 9 6 03:06:19 EST:	%BAC-	RDU-	5	0573:	Initialized CableHome WAN-MAN defaults
bac.example.com:	2007 9 6 03:06:19 EST:	%BAC-	RDU-	5	0572:	Initialized PacketCable defaults
bac.example.com:	2007 9 6 03:06:19 EST:	%BAC-	RDU-	5	0569:	Created default admin user
bac.example.com:	2007 9 6 03:06:20 EST:	%BAC-	RDU-	5	0575:	Database initialization completed in [471] msec
bac.example.com:	2007 9 6 03:06:25 EST:	%BAC-	RDU-	3	0015:	Unable to locate manifest file
bac.example.com:	2007 9 6 03:06:28 EST:	%BAC-	RDU-	3	0280:	Command error

重大度のレベルの設定

RDU と DPE のログの重大度のレベルは、いずれも特定の要件に合わせて設定できます。たとえば、RDU の重大度のレベルを「警告」、DPE の重大度のレベルを「アラート」に設定できます。

ログ メッセージは、特定のイベントの発生に基づいて記述されます。イベントが発生するたびに、該当するログ メッセージと重大度のレベルが割り当てられます。重大度のレベルが設定したレベル以下であれば、メッセージがログに書き込まれます。レベルが設定した値より高い場合、メッセージはログに書き込まれません。

たとえば、ログ レベルが 4（警告）に設定されているとします。ログ ファイルには、ログ レベルが 4 以下に設定されているイベントの生成するメッセージがすべて書き込まれます。ログ レベルが 6（情報）に設定されている場合、ログ ファイルにはすべてのメッセージが書き込まれます。したがって、ログ レベルを高く設定するほど、ログ ファイルのサイズは大きくなります。



(注)

KDC は、このログ ファイルでは考慮されません。

DPE に対する重大度のレベルを設定するには、DPE コマンドラインから **log level** コマンドを使用します。詳細については、『Cisco Broadband Access Center DPE CLI Reference 4.0』を参照してください。

RDU でのログ レベル ツールを設定するには、P.10-5 の「RDU ログ レベル ツールの使用方法」を参照してください。

ログ ファイルの循環

すべてのログ ファイルには、設定済みの最大ファイル サイズに基づいて番号が付けられ、ロールオーバーされます。デフォルトの最大ファイル サイズは 25 MB です (Application Programming Interface (API; アプリケーション プログラミング インターフェイス) から最大ファイル サイズを設定するには、*ServerDefaultsKeys.SERVER_LOG_MAXSIZE* プロパティを使用します)。ログ ファイルが設定済みの制限に達すると、データは別のファイルにロールオーバーされます。このファイルの名前は、*XXX.N.log* という形式で変更されます。内容は次のとおりです。

- *XXX* : ログ ファイルの名前を指定します。
- *N* : 1 ~ 200 のいずれかの値を示します。



(注) RDU サーバと DPE サーバは、一時に最大 200 ログ ファイルを保存します。これらのサーバのログ ファイルのリストについては、後続の項を参照してください。

たとえば、*rdu.log* が 25 MB の制限に達すると、このファイルの名前は *rdu.1.log* に変更されます。ファイルのサイズが 25 MB 増えるたびに、最新のファイルの名前は *rdu.2.log*、*rdu.3.log* のように変更されます。したがって、*rdu.4.log* ファイルには、*rdu.7.log* より新しいデータが含まれます。ただし、最新のログ情報が保存されているのは、常に *rdu.log* です。

RDU のログ

RDU には次の 2 つのログがあり、*BPR_DATA/rdu/logs* ディレクトリで保持されます。

- *rdu.log* : 設定されたデフォルトの重大度のレベルに従って、RDU 処理を記録します。(デフォルトのログ レベルの設定方法については、P.10-6 の「RDU ログ レベルの設定」を参照してください)。
- *audit.log* : BAC の設定または機能に対して行われた高いレベルの変更が記録されます。このような変更を行ったユーザも記録されます。

情報メッセージ (6 : 情報) のロギングをイネーブルにすると、RDU はバッチ処理操作を公開する追加のメッセージを記録します。これらのメッセージには、経過時間とレートに関する情報も含まれます。

rdu.log ファイルの表示

rdu.log ファイルを表示するには、任意のテキスト エディタを使用できます。また、このログ ファイルは、管理者のユーザ インターフェイスからも表示できます。

ファイルを表示するには、次の手順に従います。

ステップ 1 Servers の下の RDU タブを選択します。

View Regional Distribution Unit Details ページが表示されます。

ステップ 2 RDU Log File に対応する View Details アイコン (🔍) をクリックします。

View Log File Contents ページが表示され、*rdu.log* からのデータが示されます。

audit.log ファイルの表示

audit.log ファイルを表示するには、任意のテキストエディタを使用できます。また、このログファイルは、管理者のユーザ インターフェイスからも表示できます。

ファイルを表示するには、次の手順に従います。

ステップ 1 Servers の下の RDU タブを選択します。

View Regional Distribution Unit Details ページが表示されます。

ステップ 2 Audit Log File に対応する View Details アイコンをクリックします。

View Log File Contents ページが表示され、*audit.log* からのデータが示されます。

RDU ログ レベル ツールの使用方法

RDU ログ レベル ツールを使用して、コマンドラインから RDU の現在のログ レベルを変更します。**setLogLevel.sh** コマンドを使用します。このツールは *BPR_HOME/rdu/bin* ディレクトリにあります。

表 10-2 に利用可能な重大度のレベルとログがイネーブルになっているときにログ ファイルに書き込まれるメッセージのタイプを示します。

表 10-2 ログ レベル

ログ レベル	説明
0 : 緊急	システムが不安定です。すべての緊急メッセージを保存するように、ロギング機能を設定します。
1 : アラート	すぐに対応が必要です。すぐに対応が必要なすべてのアクティビティ、およびさらに深刻な活動を保存するように、ロギング機能を設定します。
2 : クリティカル	クリティカルな状態が存在します。すべてのエラー メッセージ、およびさらに深刻なメッセージを保存するように、ロギング機能を設定します。
3 : エラー	エラー状態が存在します。すべてのエラー メッセージ、およびさらに深刻なメッセージを保存するように、ロギング機能を設定します。
4 : 警告	警告状態が存在します。すべての警告メッセージ、およびさらに深刻なメッセージを保存するように、ロギング機能を設定します。
5 : 通知	通常ですが、重大な状態が存在します。すべての通知メッセージ、およびさらに深刻なメッセージを保存するように、ロギング機能を設定します。
6 : 情報	情報メッセージ。利用可能なすべてのロギング メッセージを保存するように、ロギング機能を設定します。



(注) 7 (デバッグ) として知られるもう 1 つのレベルは、シスコでデバッグの目的にのみ使用されます。Cisco TAC で指示された場合を除き、このレベルは使用しないようにしてください。

安定した動作状態を維持するためには、RDU 重大度のレベルを警告レベルのままにすることをお勧めします。デバッグ動作中に安定した状態パフォーマンスを維持する必要がある場合は、情報レベルを注意して使用することをお勧めします。情報レベルで実行すると大量のログ エントリが作成され、このことがパフォーマンスに悪影響を与える可能性があるため、注意が必要です。



(注)

ログ レベル ツールを実行するには、RDU プロセスが稼働している必要があります。また、**setLogLevel.sh** コマンドを使用してこのツールを実行する特権も必要です。

シンタックスの説明

setLogLevel.sh *[-0..6] [-help] [-show] [-default] [-debug]*

- **-[0..6]** : 使用する重大度のレベルを示します。利用可能なレベルのリストについては、[表 10-2](#) を参照してください。
- **-help** : ツールのヘルプを表示します。
- **-show** : RDU サーバの現在の重大度のレベル設定を表示します。
- **-default** : RDU をインストール デフォルト レベルの 5 (通知) に設定します。
- **-debug** : RDU サーバのカテゴリのトレースをイネーブルまたはディセーブルにするように、対話モードを設定します。



(注)

シスコのサポート スタッフの指示があった場合にのみ、デバッグ設定をイネーブルにしてください。

このツールを使用して、次の機能も実行できます。

- [RDU ログ レベルの設定 \(P.10-6\)](#)
- [RDU の現在のログ レベルの表示 \(P.10-7\)](#)

RDU ログ レベルの設定

このツールを使用して、ロギング レベルをある値から別の値に変更できます。次の例では、RDU ログ レベルを警告レベル (**setLogLevel.sh** コマンドでは数値 4 で示されるレベル) に設定する方法を示します。実際のログ レベル設定は手順にとって重要ではないので、必要に応じて読み替えてください。

この項で示している例は、RDU サーバが稼働中で、RDU のユーザ名が **admin**、パスワードが **changeme** であることを想定しています。

RDU ログ レベルを設定するには、次の手順に従います。

ステップ 1 *BPR_HOME/rdu/bin* にディレクトリを変更します。

ステップ 2 次のコマンドを使用して、RDU ログ レベル ツールを実行します。

```
# setLogLevel.sh 4
```

次のプロンプトが表示されます。

```
Please type RDU username:
```

ステップ 3 RDU ユーザ名を入力します。この例では、デフォルト ユーザ名 (**admin**) を使用します。

```
Please type RDU username: admin
```

次のプロンプトが表示されます。

```
Please type RDU password:
```

- ステップ 4** RDU の RDU パスワードを入力します。この例では、デフォルト パスワード (**changeme**) を使用します。

```
Please type RDU password: changeme
```

次のメッセージが表示され、ログ レベルが変更されたことが通知されます。この例では、レベル 5 (通知) から 4 (警告) に変更されました。

```
RDU Log level was changed from 5 (notification) to 4 (warning).
```

RDU の現在のログ レベルの表示

このツールを使用して、ロギング レベルの値を変更する前に、RDU ログを表示し、設定されている値を判別できます。

この項で示している例は、次のことを前提としています。

- RDU サーバが稼動中である。
- RDU のユーザ名が **admin** である。
- パスワードが **changeme** である。

RDU の現在のロギング レベルを表示するには、次の手順に従います。

-
- ステップ 1** `BPR_HOME/rdu/bin` にディレクトリを変更します。

- ステップ 2** 次のコマンドを実行します。

```
# setLogLevel.sh -show
```

次のプロンプトが表示されます。

```
Please type RDU username:
```

- ステップ 3** RDU ユーザ名 (**admin**) を入力し、**Enter** キーを押します。

```
Please type RDU username: admin
```

次のプロンプトが表示されます。

```
Please type RDU password:
```

- ステップ 4** RDU パスワード (**changeme**) を入力し、**Enter** キーを押します。

```
Please type RDU password: changeme
```

次のメッセージが表示されます。

```
The logging is currently set at level: 4 (warning)  
All tracing is currently disabled.
```

DPE のログ

DPE は *BPR_DATA/dpe/logs* ディレクトリに *dpe.log* ファイルを保持しています。このファイルには、デフォルト レベルが設定されているすべてのイベントの記録が含まれます。システム障害が連続して起こるなど、DPE で破局的な障害が発生した場合、破局的なエラーは *rdp.log* ファイルにも記録されます。

SNMPService.logyyy.log ログ ファイルは、DPE サーバで PacketCable がイネーブルになっているときに、詳細なデバッグ情報を提供するために DPE が使用します。DPE コマンドライン インターフェイス (CLI) から **service packetcable 1..1 show snmp log** コマンドを使用して、このファイルを表示します。このファイルは *BPR_DATA/dpe/logs* ディレクトリにあります。PacketCable コマンドの使用方法については、『*Cisco Broadband Access Center DPE CLI Reference 4.0*』を参照してください。



(注)

PacketCable ロギング メッセージは *dpe.log* ファイルに送信され、詳細な SNMP デバッグは *SNMPService.logyyy.log* ファイルに送信されます。

dpe.log ファイルを表示するには、任意のテキスト ビューアを使用できます。また、DPE CLI から **show log** コマンドを使用することもできます。詳細については、『*Cisco Broadband Access Center DPE CLI Reference 4.0*』を参照してください。

さらに、BAC 管理者のユーザ インターフェイスを使用して DPE ログ ファイルを表示することもできます。

ファイルを表示するには、次の手順に従います。

ステップ 1 **Servers > DPEs** を選択します。

ステップ 2 ログ ファイルを表示する DPE のリンクをクリックします。

View Device Provisioning Engines Details ページが表示されます。

ステップ 3 *dpe.log* ファイルの内容を表示するには、Log Files 領域で DPE Log File の View Details アイコンをクリックします。

Network Registrar のログ

BAC は Cisco Network Registrar DHCP サーバ拡張からログ メッセージを生成します。DHCP サーバのログは `cnr-install-path/name_dhcp_1_log` ディレクトリにあります。`cnr-install-path` は変数で、入力する値に固有のもので、DHCP サーバのログ ファイルのデフォルトの場所は `/var/nwreg2/local/logs/name_dhcp_1_log` です。

DHCP サーバ拡張経由で出力されるログ メッセージは、拡張トレース レベルの設定に基づいています。トレース レベルで値を設定できます (表 10-3 を参照)。設定する数値が、すべての拡張の `extension-trace-level` 属性の現在の設定の数値になります。

表 10-3 DHCP サーバ拡張トレース レベル

レベル	説明
0	エラーと警告の状態を記録します。すべてのエラーと警告メッセージ、およびさらに深刻なメッセージを出力するように、拡張を設定します。
1	サーバインタラクションを記録します。DPE から取得する構成命令と RDU に転送される構成生成要求が含まれます。
2	処理の詳細を記録します。命令生成要求に転送された個々の設定コマンドと属性値が含まれます。
3	拡張デバッグの内部処理を記録します。これには、メッセージの 16 進ダンプが含まれます。
4	拡張バックグラウンド操作のデバッグを記録します。これには、DPE 状態のポーリングが含まれます。

拡張トレース レベルは、Network Registrar Web UI を使用して変更できます。レベルを変更するには、次の手順に従います。

- ステップ 1** Network Registrar のローカル Web UI を開きます。
- ステップ 2** メニューから、**DHCP**、**DHCP Server** の順にクリックします。
- ステップ 3** Local DHCP Server リンクをクリックします。
- ステップ 4** Edit DHCP Server ページで、Extensions 属性カテゴリを展開します。
- ステップ 5** `extension-trace-level` 値を設定して、**Modify Server** をクリックします。
- ステップ 6** DHCP サーバをリロードします。



(注) DHCP サーバで実行されるロギングの詳細については、『*User Guide for Cisco Network Registrar 7.0*』を参照してください。

SNMP の使用によるサーバの監視

BAC では、SNMP を使用したサーバの監視がサポートされています。具体的には、SNMP ベースの管理システムを使用して、BAC サーバの状態、ライセンスの使用状況情報、サーバ接続、およびサーバ固有の統計情報を監視できます。

SNMP エージェント

BAC では、RDU サーバおよび DPE サーバについて基本的な SNMP v2 ベースの監視がサポートされます。BAC SNMP エージェントでは SNMP 通知と SNMP トラップがサポートされます。それらをまとめて「通知」と呼びます。snmp-server CLI コマンドを使用して DPE に SNMP エージェントを設定し、SNMP 設定コマンドライン ツールを使用して RDU に SNMP エージェントを設定できます。

SNMP 設定コマンドライン ツールの詳細については、P.10-11 の「snmpAgentCfgUtil.sh ツールの使用方法」を参照してください。DPE CLI の詳細については、『Cisco Broadband Access Center DPE CLI Reference 4.0』を参照してください。

MIB のサポート

BAC では、数種類の MIB がサポートされます。表 10-4 に、各 BAC コンポーネントに対する MIB サポートの概要を示します。

表 10-4 BAC でサポートされる MIB

コンポーネント	サポート対象の MIB
DPE	CISCO-BACC-SERVER-MIB
	CISCO-BACC-DPE-MIB
RDU	CISCO-BACC-SERVER-MIB
	CISCO-BACC-RDU-MIB

SNMP エージェントは CISCO-BACC-SERVER-MIB をサポートします。この MIB は、BAC 上のすべてのサーバに共通の管理対象オブジェクトを定義します。この MIB は、同一のデバイスにインストールされている複数の BAC サーバの監視をサポートします。サーバの状態が変化するたびに ciscoBaccServerStateChanged 通知が生成されます。

RDU SNMP エージェントでは、RDU の管理対象オブジェクトを定義する CISCO-BACC-RDU-MIB がサポートされます。この MIB は、RDU の状態に関する統計情報、RDU と DPE の間および RDU と Network Registrar の間の通信インターフェイスに関する統計情報を定義します。

SNMP エージェントは cnaHealthNotif トラップを生成します。このトラップは、RDU サーバの起動、シャットダウン、障害、または終了ステータスの変化を通知します。

DPE SNMP エージェントでは、DPE にインストールされているコンポーネントの管理対象オブジェクトを定義する CISCO-BACC-DPE-MIB がサポートされます。DPE は、デバイス構成のローカルキャッシング、およびサポートされているすべてのデバイスで使用される設定ファイルを管理します。この MIB は、TFTP サーバと ToD サーバのエントリを含む、基本的な DPE 設定情報と統計情報を提供します。

SNMP エージェントは CISCO-NMS-APPL-HEALTH-MIB もサポートします。この MIB は、Cisco NMS アプリケーションのヘルス ステータスの通知と関連オブジェクトを定義します。これらの通知は、NMS アプリケーションのステータス（起動、停止、失敗、ビジー、またはアプリケーションの異常終了）を知らせるために OSS/NMS に送信されます。デフォルトの MIB は MIB-II です。



(注) すべてのオブジェクトの説明については、*BPR_HOME/rdu/mibs* ディレクトリにある対応する MIB ファイルを参照してください。

snmpAgentCfgUtil.sh ツールの使用方法

snmpAgentCfgUtil.sh ツールを使用すると、Solaris コンピュータにインストールされている SNMP エージェントを管理できます。このツールは *BPR_HOME/snmp/bin* ディレクトリにあり、これを使用して、SNMP 通知を受信する他のホストのリストにホストを追加（またはリストから削除）し、SNMP エージェント プロセスを起動および中止できます。このツールはローカル ディレクトリから実行する必要があります。



(注) Solaris コンピュータ上で動作する SNMP エージェントのデフォルト ポート番号は 8001 です。

RDU SNMP エージェントは、次の操作に使用できます。

- ホストの追加 (P.10-11)
- ホストの削除 (P.10-12)
- SNMP エージェント コミュニティの追加 (P.10-12)
- SNMP エージェント コミュニティの削除 (P.10-13)
- SNMP エージェントの開始 (P.10-13)
- SNMP エージェントの停止 (P.10-14)
- SNMP エージェント リスニング ポートの設定 (P.10-14)
- SNMP エージェントの場所の変更 (P.10-14)
- SNMP の連絡先の設定 (P.10-15)
- SNMP エージェントの設定の表示 (P.10-15)
- SNMP 通知タイプの指定 (P.10-15)

ホストの追加

SNMP エージェントから SNMP 通知を受信するホストのリストにホストアドレスを追加するには、次のコマンドを使用します。

シンタックスの説明

snmpAgentCfgUtil.sh add host ip-addr community community [udp-port port]

- *ip-addr* : 通知を送信するホストの IP アドレスを指定します。
- *community* : SNMP 通知を送信するときに使用するコミュニティ（読み取りまたは書き込み）を指定します。
- *port* : SNMP 通知の送信に使用する UDP ポートを示します。

例

```
# ./snmpAgentCfgUtil.sh add host 10.10.10.5 community trapCommunity udp-port 162
OK
Please restart [stop and start] SNMP agent.
```



(注) このコマンドを使用して加えた変更は、`/etc/init.d/bprAgent restart snmpAgent` コマンドを使用して SNMP エージェントを再起動するまで有効になりません。詳細については、P.9-2 の「BAC プロセス ウォッチドッグ」を参照してください。

ホストの削除

SNMP エージェントから SNMP 通知を受信するホストのリストからホストを削除するには、次のコマンドを使用します。

シンタックスの説明

`snmpAgentCfgUtil.sh delete host ip-addr`

`ip-addr` : ホストのリストから削除するホストの IP アドレスを指定します。

例

```
# ./snmpAgentCfgUtil.sh delete host 10.10.10.5
OK
Please restart [stop and start] SNMP agent.
```



(注) このコマンドを使用して加えた変更は、`/etc/init.d/bprAgent restart snmpAgent` コマンドを使用して SNMP エージェントを再起動するまで有効になりません。詳細については、P.9-2 の「BAC プロセス ウォッチドッグ」を参照してください。

SNMP エージェント コミュニティの追加

SNMP コミュニティ スtring を追加して、SNMP エージェントへのアクセスを許可するには、次のコマンドを使用します。

シンタックスの説明

`snmpAgentCfgUtil.sh add community string [ro | rw]`

- `string` : SNMP コミュニティを示します。
- `ro` : 読み取り専用 (`ro`) のコミュニティ スtring を割り当てます。実行できるのは 取得要求 (クエリー) だけです。`ro` コミュニティ スtring は、取得要求を許可しますが、設定操作は許可しません。NMS と管理対象デバイスは、同じコミュニティ スtring を参照する必要があります。
- `rw` : 読み取りと書き込み (`rw`) コミュニティ スtring を割り当てます。SNMP アプリケーションでは、設定操作に `rw` アクセスが必要です。`rw` コミュニティ スtring を使用すると、OID 値への書き込みアクセスがイネーブルになります。



(注) デフォルトの `ro` および `rw` コミュニティ スtring は、それぞれ `baccread` と `baccwrite` です。BAC を配備する前に、これらの値を変更することをお勧めします。

例

```
# ./snmpAgentCfgUtil.sh add community fsda54 ro
OK
Please restart [stop and start] SNMP agent.
```



(注) このコマンドを使用して加えた変更は、`/etc/init.d/bprAgent restart snmpAgent` コマンドを使用して SNMP エージェントを再起動するまで有効になりません。詳細については、P.9-2 の「BAC プロセス ウォッチドッグ」を参照してください。

SNMP エージェント コミュニティの削除

SNMP コミュニティ スtring を削除して、SNMP エージェントへのアクセスを禁止するには、次のコマンドを使用します。

シンタックスの説明 `snmpAgentCfgUtil.sh delete community string [ro | rw]`

- *string* : SNMP コミュニティを示します。
- *ro* : 指定したコミュニティが読み取り専用コミュニティであることを示します。
- *rw* : 指定したコミュニティが読み取りと書き込みコミュニティであることを示します。



(注) `ro` および `rw` コミュニティ スtring の詳細については、P.10-12 の「SNMP エージェント コミュニティの追加」を参照してください。

例

```
# ./snmpAgentCfgUtil.sh delete community fsda54 ro
OK
Please restart [stop and start] SNMP agent.
```



(注) このコマンドを使用して加えた変更は、`/etc/init.d/bprAgent restart snmpAgent` コマンドを使用して SNMP エージェントを再起動するまで有効になりません。詳細については、P.9-2 の「BAC プロセス ウォッチドッグ」を参照してください。

SNMP エージェントの開始

BAC がインストールされている Solaris コンピュータで SNMP エージェント プロセスを開始するには、次のコマンドを使用します。



(注) SNMP エージェントは、`/etc/init.d/bprAgent start snmpAgent` コマンドを使用して BAC プロセス ウォッチドッグを起動することでも開始できます。詳細については、P.9-2 の「コマンドラインからの BAC プロセス ウォッチドッグの使用法」を参照してください。

例

```
# ./snmpAgentCfgUtil.sh start
Process snmpAgent has been started
```

SNMP エージェントの停止

BAC がインストールされている Solaris コンピュータで SNMP エージェント プロセスを停止するには、次のコマンドを使用します。



(注) SNMP エージェントは、`/etc/init.d/bprAgent stop snmpAgent` コマンドを使用して BAC プロセス ウォッチドッグを起動することでも停止できます。詳細については、P.9-2 の「[コマンドラインからの BAC プロセス ウォッチドッグの使用方法](#)」を参照してください。

例

```
# ./snmpAgentCfgUtil.sh stop
Process snmpAgent has stopped
```

SNMP エージェント リスニング ポートの設定

SNMP エージェントがリスンするポート番号を指定するには、次のコマンドを使用します。RDU SNMP エージェントが使用するデフォルト ポート番号は 8001 です。

シンタックスの説明 `snmpAgentCfgUtil.sh udp-port port`

port : SNMP エージェントがリスンするポート番号を示します。

例

```
# ./snmpAgentCfgUtil.sh udp-port 8001
OK
Please restart [stop and start] SNMP agent.
```



(注) このコマンドを使用して加えた変更は、`/etc/init.d/bprAgent restart snmpAgent` コマンドを使用して SNMP エージェントを再起動するまで有効になりません。詳細については、P.9-2 の「[BAC プロセス ウォッチドッグ](#)」を参照してください。

SNMP エージェントの場所の変更

SNMP エージェントを実行するデバイスの場所を示すテキスト文字列を入力するには、次のコマンドを使用します。たとえば、このコマンドを使用してデバイスの物理的な場所を示すことができます。最大 255 文字の任意の文字列を入力できます。

シンタックスの説明 `snmpAgentCfgUtil.sh location location`

location は、エージェントの場所を示す文字列です。

例 次の例では、SNMP エージェントの物理的な場所は、rack 5D と示された装置ラックです。

```
# ./snmpAgentCfgUtil.sh location "equipmentrack5D"
OK
Please restart [stop and start] SNMP agent.
```



(注) このコマンドを使用して加えた変更は、`/etc/init.d/bprAgent restart snmpAgent` コマンドを使用して SNMP エージェントを再起動するまで有効になりません。詳細については、P.9-2 の「BAC プロセス ウォッチドッグ」を参照してください。

SNMP の連絡先の設定

SNMP エージェントの連絡担当者と、この担当者への連絡方法を示すテキスト文字列を入力するには、次のコマンドを使用します。たとえば、このコマンドを使用して、特定の担当者（電話番号を含む）を示すことができます。最大 255 文字の任意の文字列を入力できます。

シンタックスの説明 `snmpAgentCfgUtil.sh contact contact-info`

`contact-info` は、SNMP エージェントに関する連絡担当者を示す文字列です。

例

次の例では、連絡担当者の名前は Terry で、内線番号は 1234 です。

```
# ./snmpAgentCfgUtil.sh contact "Terry-ext1234"
OK
Please restart [stop and start] SNMP agent.
```



(注) このコマンドを使用して加えた変更は、`/etc/init.d/bprAgent restart snmpAgent` コマンドを使用して SNMP エージェントを再起動するまで有効になりません。詳細については、P.9-2 の「BAC プロセス ウォッチドッグ」を参照してください。

SNMP エージェントの設定の表示

現在の SNMP 設定をすべて表示するには、次のコマンドを使用します。

例

```
# ./snmpAgentCfgUtil.sh show
Location                : equipmentrack5D
Contact                  : Terry-ext1234
Port Number              : 8001
Notification Type       : trap
Notification Recipient Table :
    [ Host IP address, Community, UDP Port ]
    [ 10.10.10.5 , trapCommunity , 162 ]
Access Control Table    :
    Read Only Communities
        baccread
    Read Write Communities
        baccwrite
```

SNMP 通知タイプの指定

SNMP エージェントから送信される通知のタイプ（トラップまたは通知）を指定するには、次のコマンドを使用します。デフォルトではトラップが送信されますが、SNMP 通知を送信するようにエージェントを設定することもできます。

シンタックスの説明 `snmpAgentCfgUtil.sh inform [retries timeout] | trap`

パラメータは、リトライ間のバックオフ タイムアウトです。

例

```
# ./snmpAgentCfgUtil.sh inform retries 3 timeout 1000
OK
Please restart [stop and start] SNMP agent.
```



(注) このコマンドを使用して加えた変更は、`/etc/init.d/bprAgent restart snmpAgent` コマンドを使用して SNMP エージェントを再起動するまで有効になりません。詳細については、[P.9-2](#) の「BAC プロセス ウォッチドッグ」を参照してください。

設定内容を確認するには、`snmpAgentCfgUtil.sh show` コマンドを使用します。

```
# ./snmpAgentCfgUtil.sh show
Location                : equipmentrack5D
Contact                  : Terry-ext1234
Port Number              : 8001
Notification Type       : inform
Notification Retries    : 3
Notification Timeout    : 1000
Notification Recipient Table :
    [ Host IP address, Community, UDP Port ]
    [ 10.10.10.5 , trapCommunity , 162 ]
Access Control Table    :
    Read Only Communities
        baccread
    Read Write Communities
        baccwrite
```


サーバ状態の監視

この項では、BAC 配備内の RDU サーバおよび DPE サーバのパフォーマンスを監視する方法について説明します。監視対象のサーバは、中央 RDU サーバと DPE サーバです。

サーバ統計情報は、次の手段で確認できます。

- 管理者のユーザ インターフェイス
- DPE CLI
- RDU ログ ファイルおよび DPE ログ ファイル（管理者のユーザ インターフェイスまたは DPE CLI を使用）

管理者のユーザ インターフェイスの使用方法

管理者のユーザ インターフェイスで利用可能なサーバ統計情報を表示するには、次の手順に従います。

1. プライマリ ナビゲーション バーの **Server** タブをクリックします。

セカンダリ ナビゲーション バーに、DPEs、NRs、Provisioning Group、RDU といったオプションが表示されます。

2. 次のいずれかをクリックします。

- DPEs タブ：BAC データベースに現在登録されているすべての DPE を監視する場合
- RDU タブ：RDU の状態および統計情報を表示する場合

クリックしたタブに応じて、次のように表示されます。

- DPEs：Manage Device Provisioning Engine ページが表示されます。

このページに表示される各 DPE 名は、その DPE の詳細を表示する別ページへのリンクになっています。詳細ページを表示するには、このリンクをクリックします。

- RDU：View Regional Distribution Unit Details ページが表示されます。

DPE CLI の使用方法

DPE サーバの状態を監視するには、**show dpe** コマンドを実行して、DPE が動作しているかどうかを確認し、プロセスの状態と、DPE が動作している場合は、動作状態に関する統計情報を表示します。例 10-2 を参照してください。



(注)

このコマンドでは、DPE が正常に動作しているかどうかは示されません。プロセス自体が現在実行されていることだけが示されます。ただし、DPE が動作していれば、このコマンドで出力される統計情報を使用して、DPE が正常に要求を処理しているかどうかを判別できます。

例 10-2 show dpe の出力

この結果は、DPE が動作している場合に発生します。

```
dpe# show dpe
BAC Agent is running
Process dpe is running
Version BAC 4.0 (SOL_CBAC4_0_L_000000000000).
Caching 1 device configs and 1 external files.
0 sessions succeed and 0 sessions failed.
0 file requests succeed and 0 file requests failed.
0 immediate proxy operations received: 0 succeed, and 0 failed.
Connection status is Ready.
Running for 4 hours 30 mins 16 secs.
```

この結果は、DPE が動作していない場合に発生します。

```
dpe_host# show dpe
BAC Agent is running
Process dpe is not running
```



(注) 詳細については、『Cisco Broadband Access Center DPE CLI Reference 4.0』を参照してください。